Qt 6.8 SBOM

Software Bill of Materials

06.09.2024

About myself

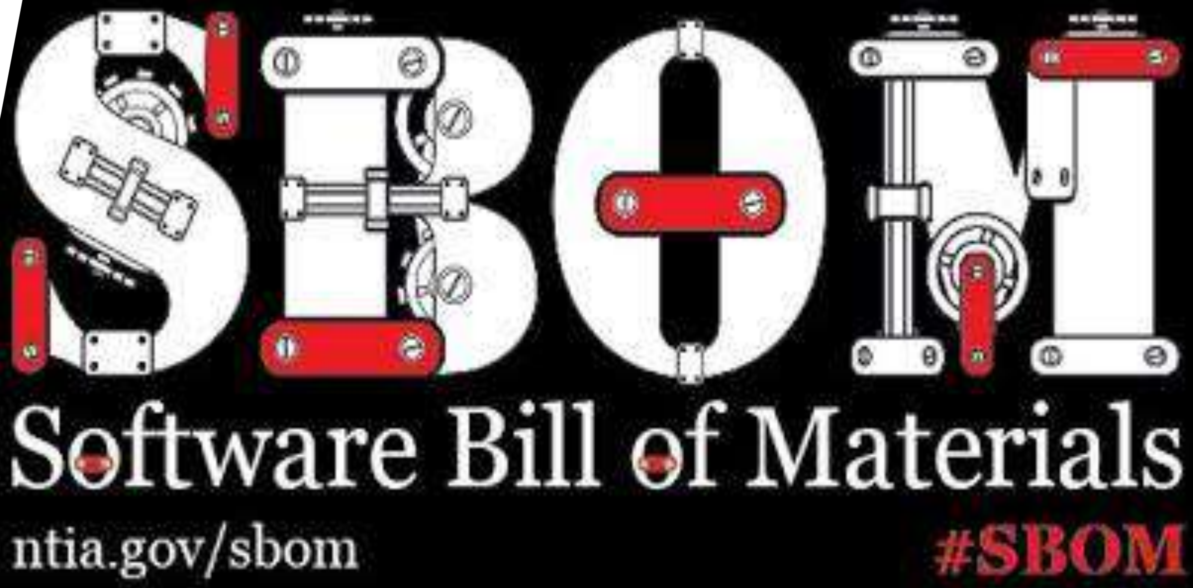
Alexandru Croitor <alexandru.croitor@qt.io>

Software Engineer from Qt Berlin Office

Maintainer of Qt Build System

Agenda

- What is an SBOM
- Why should we care
- Qt Maintainers
- Tools
- Future work

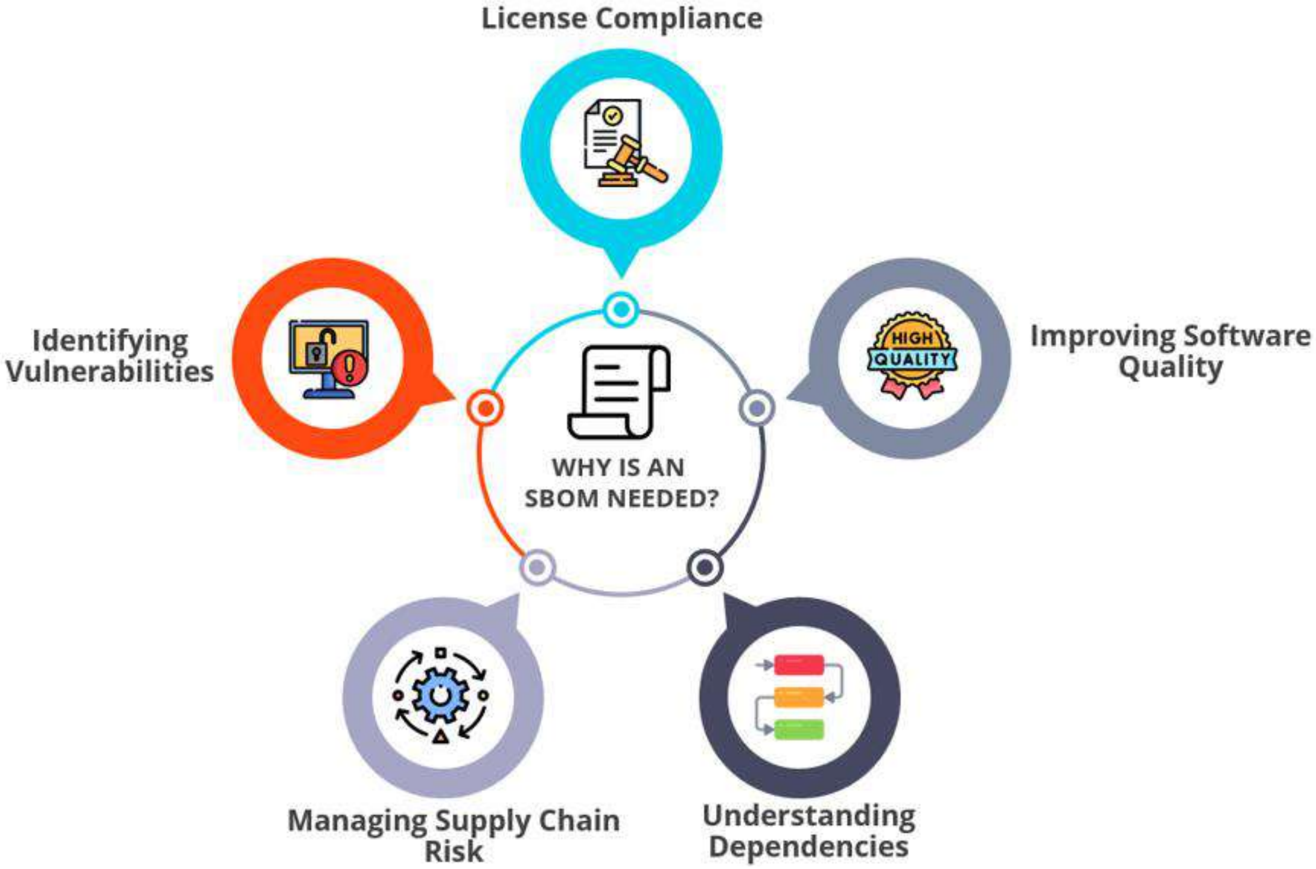


What is an SBOM?

> “A Software Bill of Materials (SBOM) is a formal record containing the details and supply chain relationships of various components used in building software.”

Why should we care?

Why should we care



License Compliance

Identifying Vulnerabilities

Improving Software Quality

WHY IS AN SBOM NEEDED?

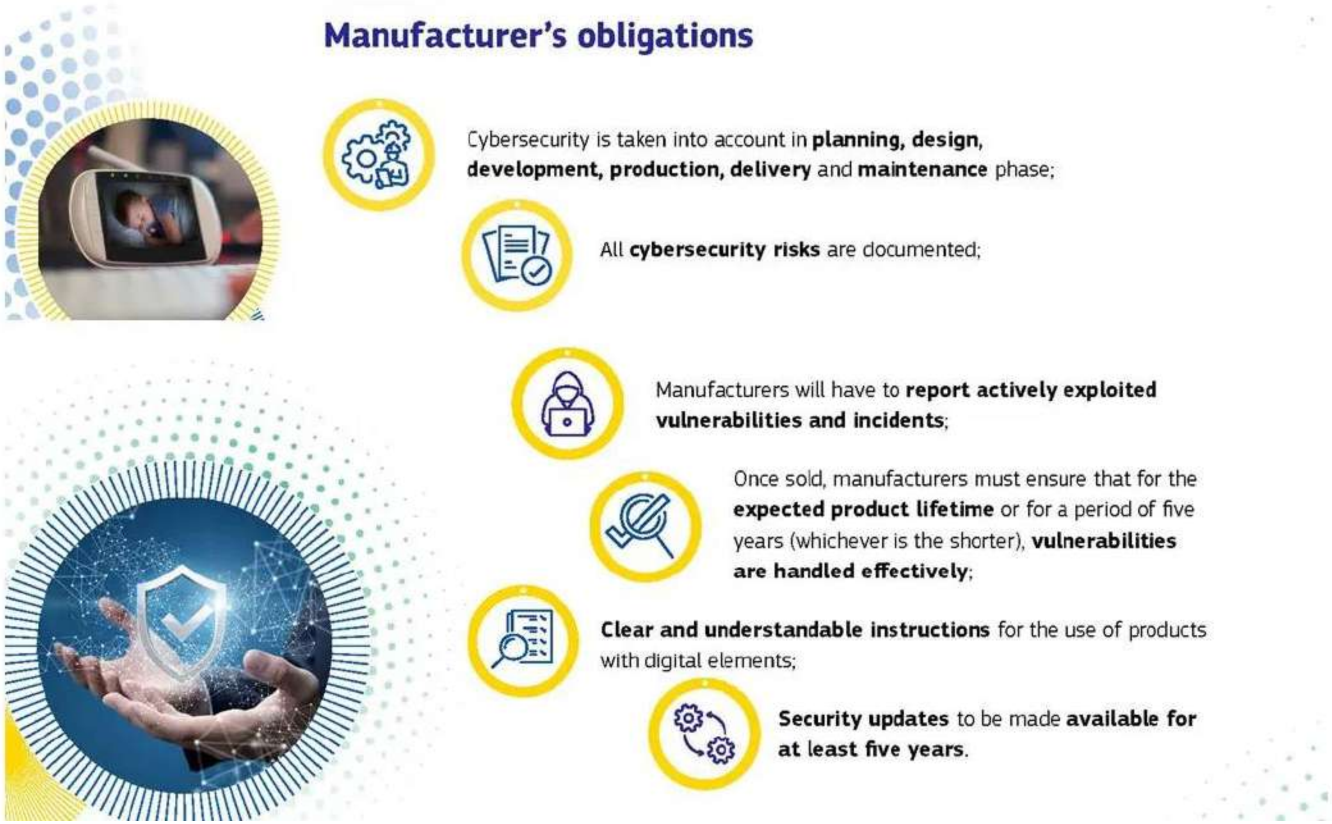
Managing Supply Chain Risk

Understanding Dependencies

But why now?

EU Cyber Resilience Act
For safer & more secure digital products
#DigitalEU #CyberSecEU

Obligations



Manufacturer's obligations

Cybersecurity is taken into account in **planning, design, development, production, delivery** and **maintenance** phase;

All **cybersecurity risks** are documented;

Manufacturers will have to **report actively exploited vulnerabilities and incidents**;

Once sold, manufacturers must ensure that for the **expected product lifetime** or for a period of five years (whichever is the shorter), **vulnerabilities are handled effectively**;

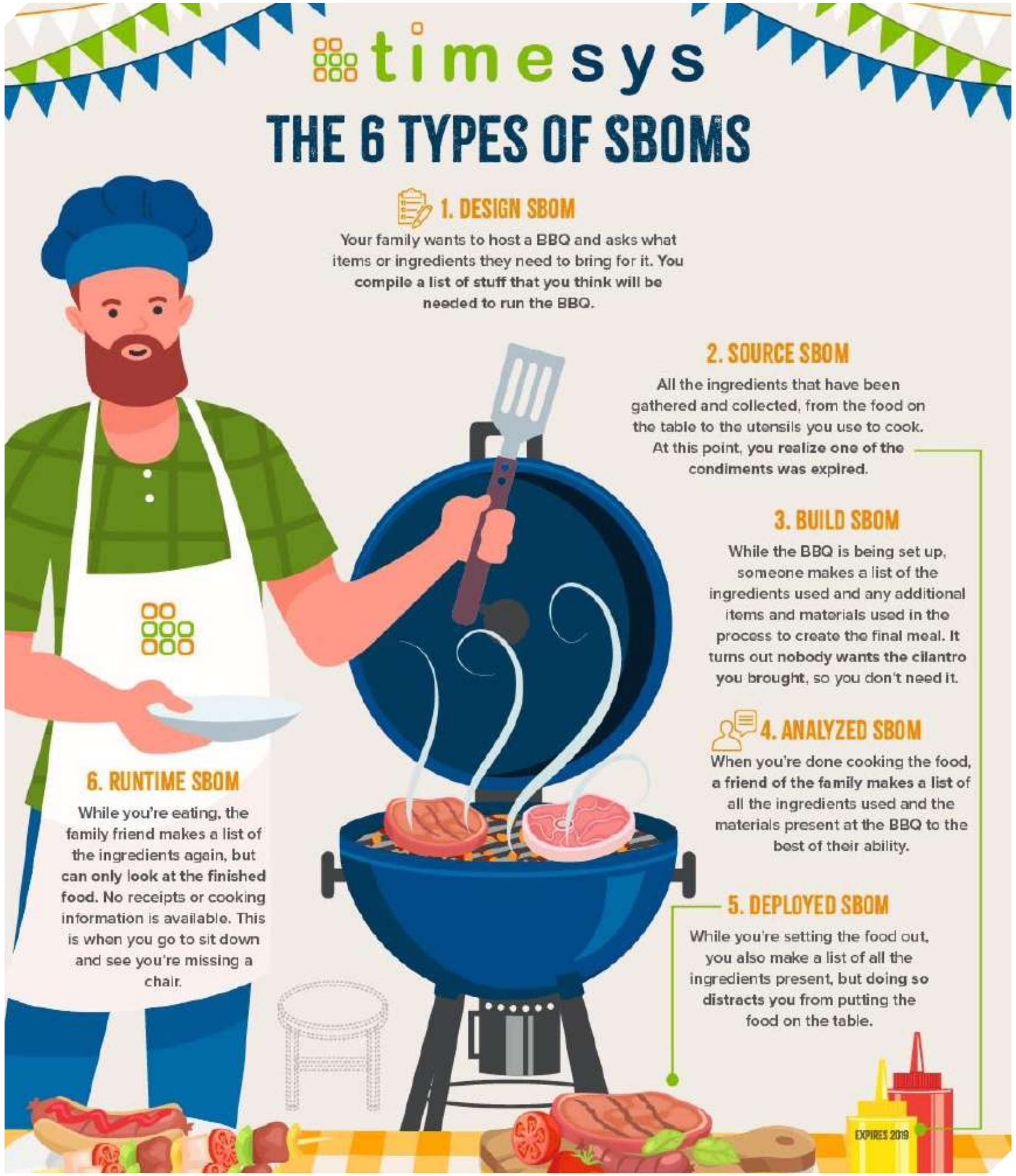
Clear and understandable instructions for the use of products with digital elements;

Security updates to be made **available for at least five years**.

What kinds of SBOMs are there?

SBOM types

- Design SBOM (from a design spec or an RFP)
- Source SBOM (from Software Composition Analysis)
- Build SBOM (generated as part of a build process)
- Analyzed SBOM (from scanning artifacts using 3rd party tools)
- Deployed SBOM (from recording installed software on a system)
- Runtime SBOM (collected by 3rd party tooling live on a system)



THE 6 TYPES OF SBOMS

1. DESIGN SBOM

Your family wants to host a BBQ and asks what items or ingredients they need to bring for it. You compile a list of stuff that you think will be needed to run the BBQ.

2. SOURCE SBOM

All the ingredients that have been gathered and collected, from the food on the table to the utensils you use to cook. At this point, you realize one of the condiments was expired.

3. BUILD SBOM

While the BBQ is being set up, someone makes a list of the ingredients used and any additional items and materials used in the process to create the final meal. It turns out nobody wants the cilantro you brought, so you don't need it.

4. ANALYZED SBOM

When you're done cooking the food, a friend of the family makes a list of all the ingredients used and the materials present at the BBQ to the best of their ability.

5. DEPLOYED SBOM

While you're setting the food out, you also make a list of all the ingredients present, but doing so distracts you from putting the food on the table.

6. RUNTIME SBOM

While you're eating, the family friend makes a list of the ingredients again, but can only look at the finished food. No receipts or cooking information is available. This is when you go to sit down and see you're missing a chair.

SBOM types

Essential for CRA

- Design SBOM (from a design spec or an RFP)
- Source SBOM (from Software Composition Analysis) <- ongoing work
- Build SBOM (generated as part of a build process) <- generated by Qt
- Analyzed SBOM (from scanning artifacts using 3rd party tools)
- Deployed SBOM (from recording installed software on a system)
- Runtime SBOM (collected by 3rd party tooling live on a system)

timesys
EXPIRES 2019

THE 6 TYPES OF SBOMS

1. DESIGN SBOM

Your family wants to host a BBQ and asks what items or ingredients they need to bring for it. You compile a list of stuff that you think will be needed to run the BBQ.

2. SOURCE SBOM

All the ingredients that have been gathered and collected, from the food on the table to the utensils you use to cook. At this point, you realize one of the condiments was expired.

3. BUILD SBOM

While the BBQ is being set up, someone makes a list of the ingredients used and any additional items and materials used in the process to create the final meal. It turns out nobody wants the cilantro you brought, so you don't need it.

4. ANALYZED SBOM

When you're done cooking the food, a friend of the family makes a list of all the ingredients used and the materials present at the BBQ to the best of their ability.

5. DEPLOYED SBOM

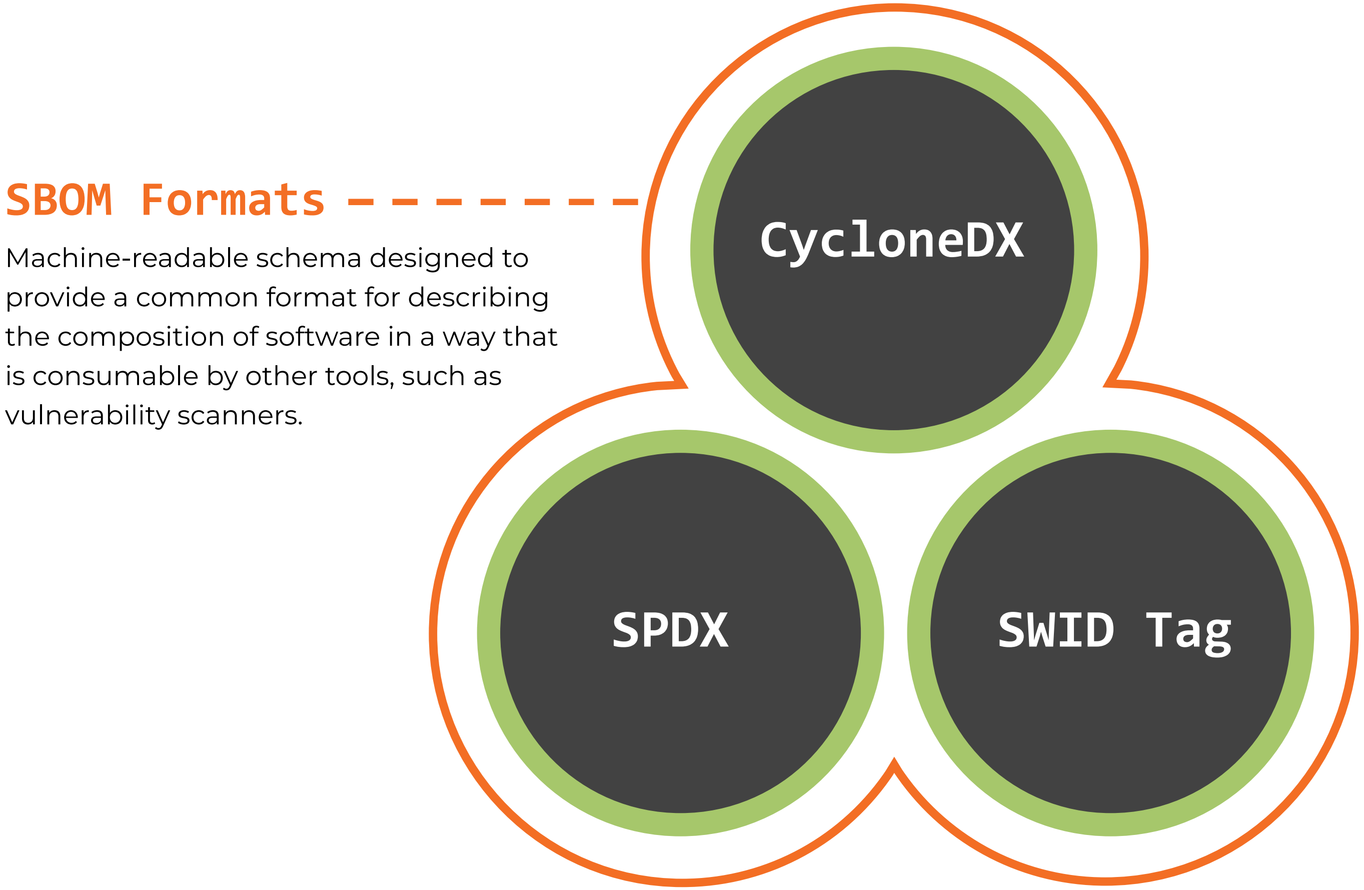
While you're setting the food out, you also make a list of all the ingredients present, but doing so distracts you from putting the food on the table.

6. RUNTIME SBOM

While you're eating, the family friend makes a list of the ingredients again, but can only look at the finished food. No receipts or cooking information is available. This is when you go to sit down and see you're missing a chair.

SBOM formats

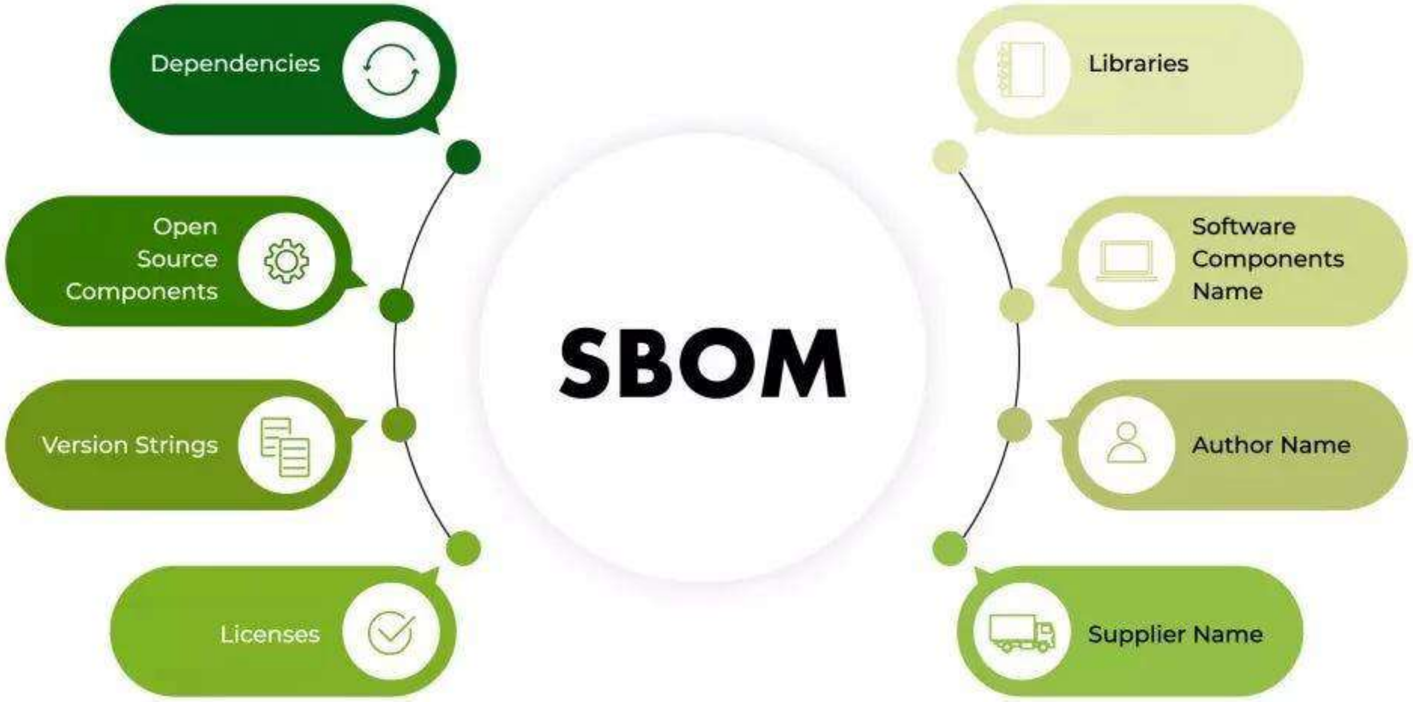
- SPDX
  - https://spdx.dev/
  - Maintained by Linux Foundation
  - Latest version v3.0
  - Most popular **v2.3** <- Generated by Qt
- CycloneDX
  - https://cyclonedx.org/
  - Maintained by OWASP
  - Latest version v1.6
- SWID by ISO / IEC



SBOM Formats

Machine-readable schema designed to provide a common format for describing the composition of software in a way that is consumable by other tools, such as vulnerability scanners.

Build SBOM


SBOM
Dependencies
Open Source Components
Version Strings
Licenses
Libraries
Software Components Name
Author Name
Supplier Name

Build Build SBOM

- Generated by Qt’s build system

- configure --sbom
- cmake --install . --component sbom

- Installs one .spdx file per qt repository

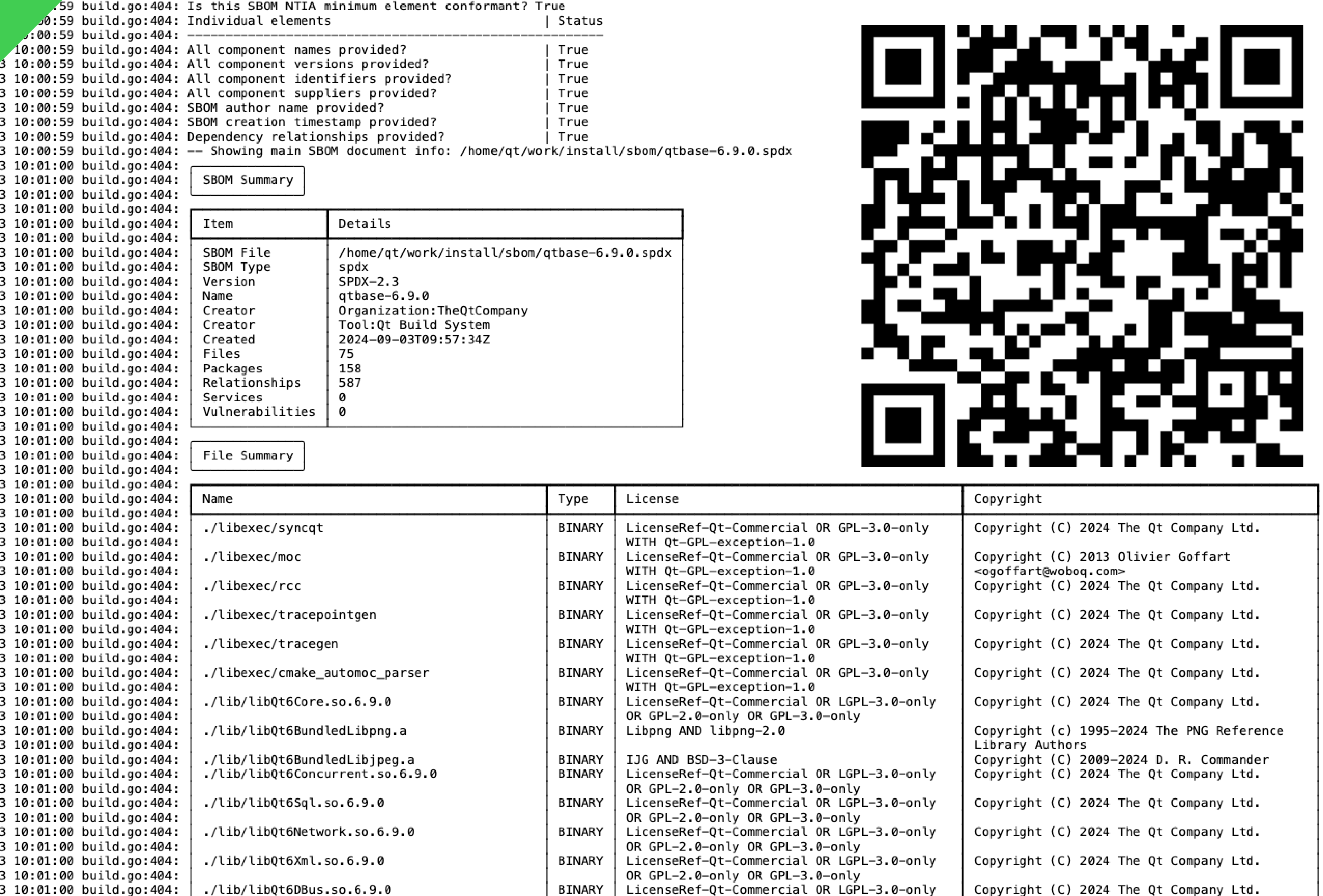
```
$ ls -alh installed/sbom
total 3840
drwxr-xr-x   4 alex  staff   128B Sep  3 17:33 .
drwxr-xr-x  22 alex  staff   704B Aug 23 12:03 ..
-rw-r--r--   1 alex  staff   721K Sep  3 17:33 qtbase-6.9.0.spdx
-rw-r--r--   1 alex  staff   1.2M Sep  3 17:33 qtbase-6.9.0.spdx.json
```

Sample Build SBOM snippet from qtbase

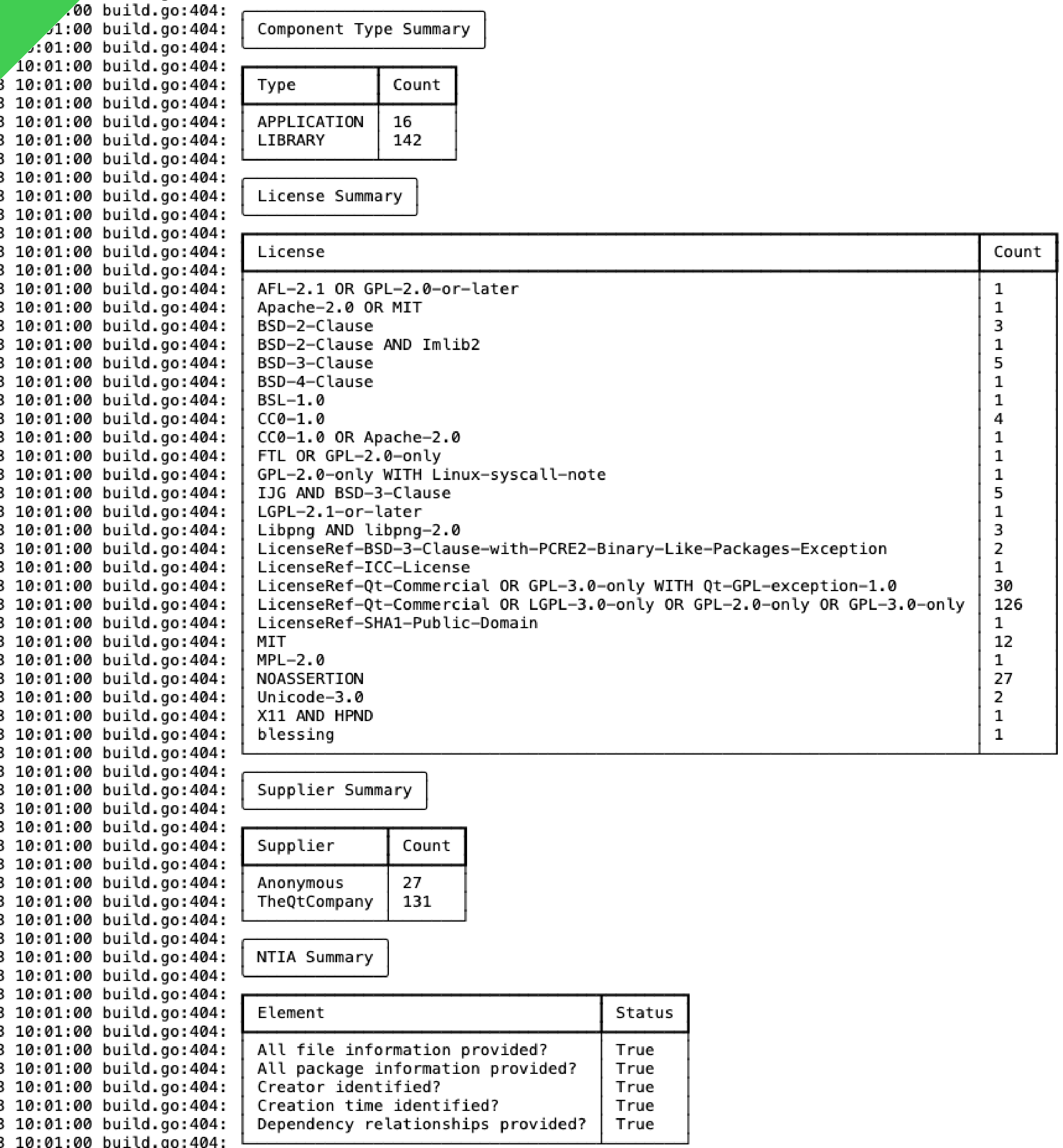
- PackageName: Gui
- SPDXID: SPDXRef-Package-qtbase-qt-module-Gui
- PackageDownloadLocation: git://code.qt.io/qt/qtbase.git@ca10f27ef6efb904a6b3392255c380e4e27ccef0
- PackageVersion: 6.9.0
- PackageSupplier: Organization: TheQtCompany
- PackageLicenseConcluded: LicenseRef-Qt-Commercial OR LGPL-3.0-only OR GPL-2.0-only OR GPL-3.0-only
- ExternalRef: PACKAGE-MANAGER purl pkg:github/qt/qtbase@ca10f27ef6e?library_name=Gui#src/gui
- ExternalRef: PACKAGE-MANAGER purl pkg:generic/TheQtCompany/qtbase-Gui@ca10f27ef6e?vcs_url=https://code.qt.io/qt/qtbase.git@ca10f27ef6e&library_name=Gui#src/gui
- PackageCopyrightText: <text>Copyright (C) 2024 The Qt Company Ltd.</text>
- PrimaryPackagePurpose: LIBRARY
- ExternalRef: SECURITY cpe23Type cpe:2.3:a:qt:qtbase:6.9.0:*:*:*:*:*:*:*
- ExternalRef: SECURITY cpe23Type cpe:2.3:a:qt:qt:6.9.0:*:*:*:*:*:*:*
- Relationship: SPDXRef-Package-qtbase-qt-module-Gui DEPENDS_ON SPDXRef-Package-qtbase-qt-module-Core
- Relationship: SPDXRef-Package-qtbase-qt-module-Gui DEPENDS_ON SPDXRef-Package-qtbase-qt-bundled-3rdparty-module-BundledLibpng
- Relationship: SPDXRef-Package-qtbase-qt-module-Gui DEPENDS_ON SPDXRef-Package-qtbase-qt-bundled-3rdparty-module-BundledHarfbuzz
- Relationship: SPDXRef-Package-qtbase-qt-module-Gui DEPENDS_ON SPDXRef-Package-qtbase-qt-3rdparty-sources-Gui-Attribution-VulkanMemoryAllocator
- Relationship: SPDXRef-Package-qtbase-qt-module-Gui DEPENDS_ON SPDXRef-Package-qtbase-qt-3rdparty-sources-Gui-Attribution-icc-sRGB-color-profile
- Relationship: SPDXRef-Package-qtbase-qt-module-Gui DEPENDS_ON SPDXRef-Package-qtbase-qt-3rdparty-sources-Gui-Attribution-md4c
- Relationship: SPDXRef-Package-qtbase-qt-module-Gui DEPENDS_ON SPDXRef-Package-qtbase-qt-3rdparty-sources-Gui-Attribution-zlib
- Relationship: SPDXRef-Package-qtbase CONTAINS SPDXRef-Package-qtbase-qt-module-Gui

Sample 3rd party snippet

- PackageName: BundledZLIB
- SPDXID: SPDXRef-Package-qtbase-qt-bundled-3rdparty-module-BundledZLIB
- PackageDownloadLocation: https://github.com/madler/zlib/releases/download/v1.3.1/zlib-1.3.1.tar.gz
- PackageVersion: 1.2.12
- PackageSupplier: Organization: TheQtCompany
- PackageLicenseConcluded: Zlib
- ExternalRef: PACKAGE-MANAGER purl pkg:github/madler/zlib@v1.2.12
- ExternalRef: PACKAGE-MANAGER purl pkg:github/qt/qtbase@ca10f27ef6e?library_name=BundledZLIB#src/3rdparty/zlib
- PackageCopyrightText: <text>(C) 1995-2024 Jean-loup Gailly and Mark Adler</text>
- PrimaryPackagePurpose: LIBRARY
- PackageComment: <text>
- Name: Data Compression Library (zlib)
- Description: zlib is a general purpose data compression library.
- Qt usage: Optionally used in Qt Core and development tools. Configure with -system-zlib to avoid.
- Information extracted from:
- /Users/alex/Dev/qt/worktrees/dev/qtbase/src/3rdparty/zlib/qt_attribution.json
- Entry index: 0
- </text>
- ExternalRef: SECURITY cpe23Type cpe:2.3:a:zlib:zlib:1.2.12:*:*:*:*:*:*:*
- Relationship: SPDXRef-Package-qtbase-qt-bundled-3rdparty-module-BundledZLIB DEPENDS_ON SPDXRef-Package-qtbase-qt-module-PlatformModuleInternal
- Relationship: SPDXRef-Package-qtbase CONTAINS SPDXRef-Package-qtbase-qt-bundled-3rdparty-module-BundledZLIB



```
 .59 build.go:404: Is this SBOM NTIA minimum element conformant? True
 0:59 build.go:404: Individual elements                            | Status
 :00:59 build.go:404: --------------------------------------------------------
 10:00:59 build.go:404: All component names provided?                  | True
3 10:00:59 build.go:404: All component versions provided?               | True
3 10:00:59 build.go:404: All component identifiers provided?            | True
3 10:00:59 build.go:404: All component suppliers provided?              | True
3 10:00:59 build.go:404: SBOM author name provided?                     | True
3 10:00:59 build.go:404: SBOM creation timestamp provided?              | True
3 10:00:59 build.go:404: Dependency relationships provided?             | True
3 10:00:59 build.go:404: -- Showing main SBOM document info: /home/qt/work/install/sbom/qtbase-6.9.0.spdx
3 10:01:00 build.go:404:
3 10:01:00 build.go:404:  SBOM Summary
3 10:01:00 build.go:404:
3 10:01:00 build.go:404:
3 10:01:00 build.go:404:  Item             Details
3 10:01:00 build.go:404:
3 10:01:00 build.go:404:  SBOM File        /home/qt/work/install/sbom/qtbase-6.9.0.spdx
3 10:01:00 build.go:404:  SBOM Type        spdx
3 10:01:00 build.go:404:  Version          SPDX-2.3
3 10:01:00 build.go:404:  Name             qtbase-6.9.0
3 10:01:00 build.go:404:  Creator          Organization:TheQtCompany
3 10:01:00 build.go:404:  Creator          Tool:Qt Build System
3 10:01:00 build.go:404:  Created          2024-09-03T09:57:34Z
3 10:01:00 build.go:404:  Files            75
3 10:01:00 build.go:404:  Packages         158
3 10:01:00 build.go:404:  Relationships    587
3 10:01:00 build.go:404:  Services         0
3 10:01:00 build.go:404:  Vulnerabilities  0
3 10:01:00 build.go:404:
3 10:01:00 build.go:404:
3 10:01:00 build.go:404:  File Summary
3 10:01:00 build.go:404:
3 10:01:00 build.go:404:
3 10:01:00 build.go:404:  Name                            Type    License                                   Copyright
3 10:01:00 build.go:404:
3 10:01:00 build.go:404:  ./libexec/syncqt                BINARY  LicenseRef-Qt-Commercial OR GPL-3.0-only  Copyright (C) 2024 The Qt Company Ltd.
3 10:01:00 build.go:404:                                          WITH Qt-GPL-exception-1.0
3 10:01:00 build.go:404:  ./libexec/moc                   BINARY  LicenseRef-Qt-Commercial OR GPL-3.0-only  Copyright (C) 2013 Olivier Goffart
3 10:01:00 build.go:404:                                          WITH Qt-GPL-exception-1.0                 <ogoffart@woboq.com>
3 10:01:00 build.go:404:  ./libexec/rcc                   BINARY  LicenseRef-Qt-Commercial OR GPL-3.0-only  Copyright (C) 2024 The Qt Company Ltd.
3 10:01:00 build.go:404:                                          WITH Qt-GPL-exception-1.0
3 10:01:00 build.go:404:  ./libexec/tracepointgen         BINARY  LicenseRef-Qt-Commercial OR GPL-3.0-only  Copyright (C) 2024 The Qt Company Ltd.
3 10:01:00 build.go:404:                                          WITH Qt-GPL-exception-1.0
3 10:01:00 build.go:404:  ./libexec/tracegen              BINARY  LicenseRef-Qt-Commercial OR GPL-3.0-only  Copyright (C) 2024 The Qt Company Ltd.
3 10:01:00 build.go:404:                                          WITH Qt-GPL-exception-1.0
3 10:01:00 build.go:404:  ./libexec/cmake_automoc_parser  BINARY  LicenseRef-Qt-Commercial OR GPL-3.0-only  Copyright (C) 2024 The Qt Company Ltd.
3 10:01:00 build.go:404:                                          WITH Qt-GPL-exception-1.0
3 10:01:00 build.go:404:  ./lib/libQt6Core.so.6.9.0       BINARY  LicenseRef-Qt-Commercial OR LGPL-3.0-only Copyright (C) 2024 The Qt Company Ltd.
3 10:01:00 build.go:404:                                          OR GPL-2.0-only OR GPL-3.0-only
3 10:01:00 build.go:404:  ./lib/libQt6BundledLibpng.a     BINARY  Libpng AND libpng-2.0                     Copyright (c) 1995-2024 The PNG Reference
3 10:01:00 build.go:404:                                                                                    Library Authors
3 10:01:00 build.go:404:  ./lib/libQt6BundledLibjpeg.a    BINARY  IJG AND BSD-3-Clause                      Copyright (C) 2009-2024 D. R. Commander
3 10:01:00 build.go:404:  ./lib/libQt6Concurrent.so.6.9.0 BINARY  LicenseRef-Qt-Commercial OR LGPL-3.0-only Copyright (C) 2024 The Qt Company Ltd.
3 10:01:00 build.go:404:                                          OR GPL-2.0-only OR GPL-3.0-only
3 10:01:00 build.go:404:  ./lib/libQt6Sql.so.6.9.0        BINARY  LicenseRef-Qt-Commercial OR LGPL-3.0-only Copyright (C) 2024 The Qt Company Ltd.
3 10:01:00 build.go:404:                                          OR GPL-2.0-only OR GPL-3.0-only
3 10:01:00 build.go:404:  ./lib/libQt6Network.so.6.9.0    BINARY  LicenseRef-Qt-Commercial OR LGPL-3.0-only Copyright (C) 2024 The Qt Company Ltd.
3 10:01:00 build.go:404:                                          OR GPL-2.0-only OR GPL-3.0-only
3 10:01:00 build.go:404:  ./lib/libQt6Xml.so.6.9.0        BINARY  LicenseRef-Qt-Commercial OR LGPL-3.0-only Copyright (C) 2024 The Qt Company Ltd.
3 10:01:00 build.go:404:                                          OR GPL-2.0-only OR GPL-3.0-only
3 10:01:00 build.go:404:  ./lib/libQt6DBus.so.6.9.0       BINARY  LicenseRef-Qt-Commercial OR LGPL-3.0-only Copyright (C) 2024 The Qt Company Ltd.
```

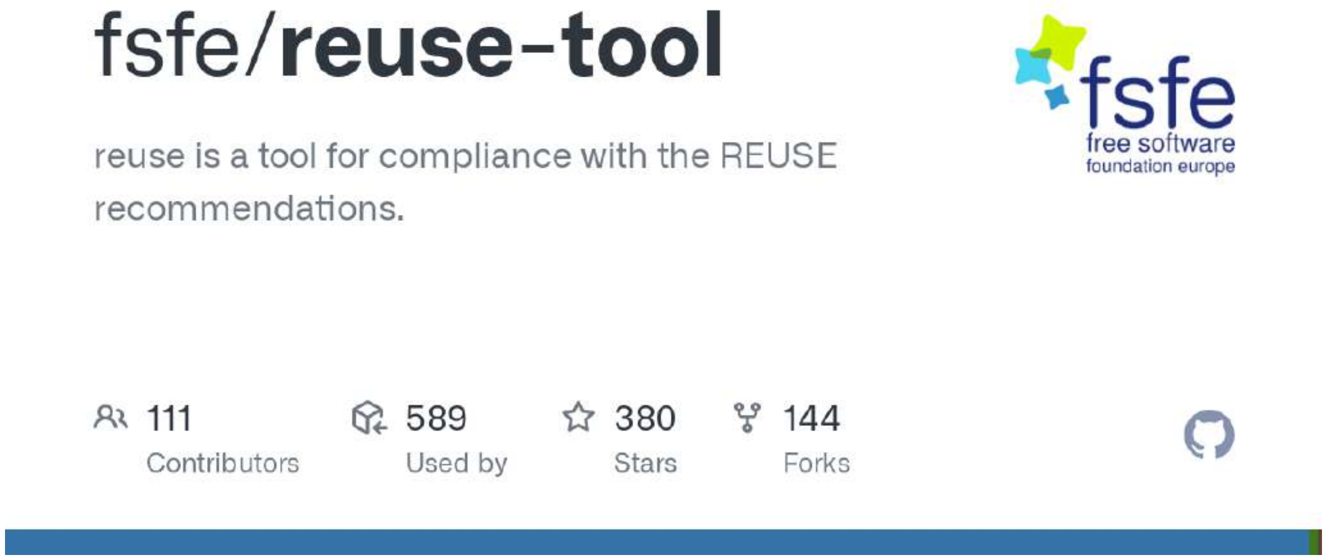


```
       :00 build.go:404: ┌────────────────────────┐
     01:00 build.go:404: │ Component Type Summary │
   0:01:00 build.go:404: └────────────────────────┘
  10:01:00 build.go:404: ┌─────────────┬───────┐
3 10:01:00 build.go:404: │ Type        │ Count │
3 10:01:00 build.go:404: ├─────────────┼───────┤
3 10:01:00 build.go:404: │ APPLICATION │ 16    │
3 10:01:00 build.go:404: │ LIBRARY     │ 142   │
3 10:01:00 build.go:404: └─────────────┴───────┘
3 10:01:00 build.go:404: ┌─────────────────┐
3 10:01:00 build.go:404: │ License Summary │
3 10:01:00 build.go:404: └─────────────────┘
3 10:01:00 build.go:404: ┌───────────────────────────────────────────────────────────────────────────┬───────┐
3 10:01:00 build.go:404: │ License                                                                   │ Count │
3 10:01:00 build.go:404: ├───────────────────────────────────────────────────────────────────────────┼───────┤
3 10:01:00 build.go:404: │ AFL-2.1 OR GPL-2.0-or-later                                               │ 1     │
3 10:01:00 build.go:404: │ Apache-2.0 OR MIT                                                         │ 1     │
3 10:01:00 build.go:404: │ BSD-2-Clause                                                              │ 3     │
3 10:01:00 build.go:404: │ BSD-2-Clause AND Imlib2                                                   │ 1     │
3 10:01:00 build.go:404: │ BSD-3-Clause                                                              │ 5     │
3 10:01:00 build.go:404: │ BSD-4-Clause                                                              │ 1     │
3 10:01:00 build.go:404: │ BSL-1.0                                                                   │ 1     │
3 10:01:00 build.go:404: │ CC0-1.0                                                                   │ 4     │
3 10:01:00 build.go:404: │ CC0-1.0 OR Apache-2.0                                                     │ 1     │
3 10:01:00 build.go:404: │ FTL OR GPL-2.0-only                                                       │ 1     │
3 10:01:00 build.go:404: │ GPL-2.0-only WITH Linux-syscall-note                                      │ 1     │
3 10:01:00 build.go:404: │ IJG AND BSD-3-Clause                                                      │ 5     │
3 10:01:00 build.go:404: │ LGPL-2.1-or-later                                                         │ 1     │
3 10:01:00 build.go:404: │ Libpng AND libpng-2.0                                                     │ 3     │
3 10:01:00 build.go:404: │ LicenseRef-BSD-3-Clause-with-PCRE2-Binary-Like-Packages-Exception         │ 2     │
3 10:01:00 build.go:404: │ LicenseRef-ICC-License                                                    │ 1     │
3 10:01:00 build.go:404: │ LicenseRef-Qt-Commercial OR GPL-3.0-only WITH Qt-GPL-exception-1.0        │ 30    │
3 10:01:00 build.go:404: │ LicenseRef-Qt-Commercial OR LGPL-3.0-only OR GPL-2.0-only OR GPL-3.0-only │ 126   │
3 10:01:00 build.go:404: │ LicenseRef-SHA1-Public-Domain                                             │ 1     │
3 10:01:00 build.go:404: │ MIT                                                                       │ 12    │
3 10:01:00 build.go:404: │ MPL-2.0                                                                   │ 1     │
3 10:01:00 build.go:404: │ NOASSERTION                                                               │ 27    │
3 10:01:00 build.go:404: │ Unicode-3.0                                                               │ 2     │
3 10:01:00 build.go:404: │ X11 AND HPND                                                              │ 1     │
3 10:01:00 build.go:404: │ blessing                                                                  │ 1     │
3 10:01:00 build.go:404: └───────────────────────────────────────────────────────────────────────────┴───────┘
3 10:01:00 build.go:404: ┌──────────────────┐
3 10:01:00 build.go:404: │ Supplier Summary │
3 10:01:00 build.go:404: └──────────────────┘
3 10:01:00 build.go:404: ┌──────────────┬───────┐
3 10:01:00 build.go:404: │ Supplier     │ Count │
3 10:01:00 build.go:404: ├──────────────┼───────┤
3 10:01:00 build.go:404: │ Anonymous    │ 27    │
3 10:01:00 build.go:404: │ TheQtCompany │ 131   │
3 10:01:00 build.go:404: └──────────────┴───────┘
3 10:01:00 build.go:404: ┌──────────────┐
3 10:01:00 build.go:404: │ NTIA Summary │
3 10:01:00 build.go:404: └──────────────┘
3 10:01:00 build.go:404: ┌────────────────────────────────────┬────────┐
3 10:01:00 build.go:404: │ Element                            │ Status │
3 10:01:00 build.go:404: ├────────────────────────────────────┼────────┤
3 10:01:00 build.go:404: │ All file information provided?     │ True   │
3 10:01:00 build.go:404: │ All package information provided?  │ True   │
3 10:01:00 build.go:404: │ Creator identified?                │ True   │
3 10:01:00 build.go:404: │ Creation time identified?          │ True   │
3 10:01:00 build.go:404: │ Dependency relationships provided? │ True   │
3 10:01:00 build.go:404: └────────────────────────────────────┴────────┘
```

Source SBOM

Source SBOM via REUSE software

- REUSE Software
  - https://reuse.software/
  - Maintained by FSFE
  - Spec for annotating source files with license and copyright info
  - Either as comment headers or external REUSE.toml file
  - Latest version v3.2
  - Provides tool to lint and generate source SBOM
  - Qt REUSE-ification PoC in progress
- Why?
  - Complements Build SBOM nicely by cross-referencing source files that were used for the build, for license and copyright info



fsfe/**reuse-tool**

reuse is a tool for compliance with the REUSE recommendations.

111 Contributors

589 Used by

380 Stars

144 Forks

REUSE.toml sample

- src/corelib/kernel/qiterable.h

- // Copyright (C) 2020 The Qt Company Ltd.
- // SPDX-License-Identifier: LicenseRef-Qt-Commercial OR LGPL-3.0-only OR GPL-2.0-only OR GPL-3.0-only

- src/3rdparty/zlib/REUSE.toml

- version = 1

- [[annotations]]
- path = ["**"]
- precedence = "closest"
- SPDX-FileCopyrightText = ["(C) 1995-2024 Jean-loup Gailly and Mark Adler"]
- SPDX-License-Identifier = "Zlib"

Source SBOM generated by REUSE tool

- SPDXVersion: SPDX-2.1
- DataLicense: CC0-1.0
- SPDXID: SPDXRef-DOCUMENT
- DocumentName: qtbase
- DocumentNamespace: http://spdx.org/spdxdocs/spdx-v2.1-63fc9b58-9724-4dc0-b7c0-9ab404c9c715
- Creator: Person: Anonymous ()
- Creator: Organization: Anonymous ()
- Creator: Tool: reuse-4.0.3
- Created: 2024-09-04T09:36:30Z
- CreatorComment: <text>This document was created automatically using available reuse information consistent with REUSE.</text>
- Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-fbd0885568e50f6a4ff28e2473e0b11e
- …..
- FileName: ./src/corelib/kernel/qiterable.h
- SPDXID: SPDXRef-1aa25c082a262d7b8bc81283c3163bef
- FileChecksum: SHA1: c89f41cad97974e2644cbdfddf6bf4fb7fef0337
- LicenseConcluded: NOASSERTION
- LicenseInfoInFile: GPL-2.0-only
- LicenseInfoInFile: GPL-3.0-only
- LicenseInfoInFile: LGPL-3.0-only
- LicenseInfoInFile: LicenseRef-Qt-Commercial
- FileCopyrightText: <text>Copyright (C) 2020 The Qt Company Ltd.</text>

REUSE lint

```
-- Running 'reuse lint' in '/Users/alex/Dev/qt/worktrees/dev/qtbase'.

# SUMMARY
* Bad licenses: 0
* Deprecated licenses: 0
* Licenses without file extension: 0
* Missing licenses: 0
* Unused licenses: 0
* Used licenses: MPL-2.0, BSD-4-Clause, Unicode-3.0, GPL-2.0-or-later, libpng-2.0, GPL-3.0-only, Bitstream-Vera, GPL-2.0-only, MIT, MIT-open-group, SPL-1.0, Apache-2.0, Qt-GPL-exception-1.0, blessing, AFL-2.1, LicenseRef-BSD-3-Clause-with-PCRE2-Binary-Like-Packages-Exception, BSL-1.0, Imlib2, BSD-3-Clause, HPND, IJG, X11, LicenseRef-ICC-License, GFDL-1.3-no-invariants-only, Zlib, Libpng, LicenseRef-Lcs-Telegraphics, BSD-2-Clause, MIT-Khronos-old, LicenseRef-SHA1-Public-Domain, LGPL-3.0-only, FTL, Linux-syscall-note, CC0-1.0, IPL-1.0, LicenseRef-Qt-Commercial, Xerox
* Read errors: 0
* Files with copyright information: 22197 / 22197
* Files with license information: 22197 / 22197

Congratulations! Your project is compliant with version 3.2 of the REUSE Specification :-)
```

What Qt maintainers need to know

What Qt maintainers need to know

- https://wiki.qt.io/SBOM#For_Maintainers
- Annotate modules with correct license
- Annotate usage of 3rd party sources
- Keep qt_attribution.json CPE / PURL up-to-date

Module licensing

- Default module license is “*LicenseRef-Qt-Commercial OR LGPL-3.0-only OR GPL-2.0-only OR GPL-3.0*”

- Modify module CMakeLists.txt to customize the license

```
# inside src/CMakeLists.txt
set(QT_SBOM_DEFAULT_QT_LICENSE_ID_LIBRARIES "QT_COMMERCIAL_OR_GPL3")
set(QT_SBOM_DEFAULT_QT_LICENSE_ID_EXECUTABLES "QT_COMMERCIAL_OR_GPL3")
```

3rd party usage annotation

- qt_internal_extend_target(Network
- CONDITION
- NOT QT_FEATURE_system_zlib
- INCLUDE_DIRECTORIES
- ../3rdparty/zlib/src
- ATTRIBUTION_FILE_DIR_PATHS
- ../3rdparty/zlib
- ../3rdparty/openssl)

qt_attribution.json CPE / PURL

- "PURL": "pkg:github/PCRE2Project/pcre2@pcre2-10.44",
- "CPE": "cpe:2.3:a:pcre:pcre2:10.44:*:*:*:*:*:*:*",

- "PURL": "pkg:generic/xcb-xinput?download_url=http://xcb.freedesktop.org/",

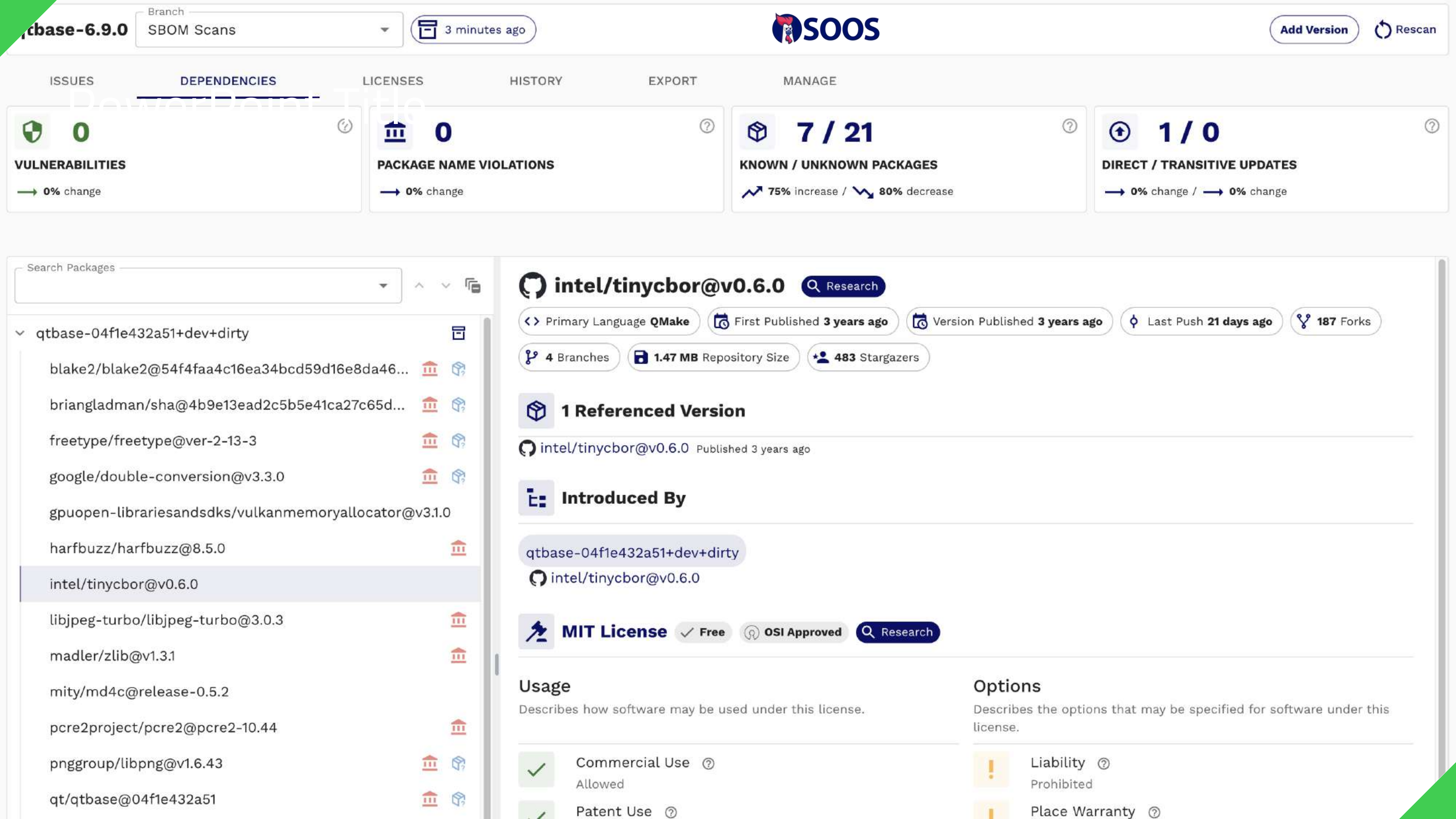
- "PURL": "pkg:github/apache/tika@5ea8bbf1644a593ed22ee5c7608ba33aff949d5d#tika-core/src/main/resources/org/apache/tika/mime/tika-mimetypes.xml",
- "CPE": "cpe:2.3:a:apache:tika:*:*:*:*:*:*:*:*",

Tools

Tools

- SOOS
  - https://soos.io/
  - Commercial, paid
- Dependency Track
  - https://github.com/DependencyTrack/dependency-track
  - Open Source, free
- Intel cve-bin-tool
  - https://github.com/intel/cve-bin-tool
  - Open Source, free

intel/**cve-bin-tool**



tbase-6.9.0

Branch: SBOM Scans

3 minutes ago

0 VULNERABILITIES — 0% change

0 PACKAGE NAME VIOLATIONS — 0% change

7 / 21 KNOWN / UNKNOWN PACKAGES — 75% increase / 80% decrease

1 / 0 DIRECT / TRANSITIVE UPDATES — 0% change / 0% change

Search Packages

qtbase-04f1e432a51+dev+dirty
- blake2/blake2@54f4faa4c16ea34bcd59d16e8da46...
- briangladman/sha@4b9e13ead2c5b5e41ca27c65d...
- freetype/freetype@ver-2-13-3
- google/double-conversion@v3.3.0
- gpuopen-librariesandsdks/vulkanmemoryallocator@v3.1.0
- harfbuzz/harfbuzz@8.5.0
- intel/tinycbor@v0.6.0
- libjpeg-turbo/libjpeg-turbo@3.0.3
- madler/zlib@v1.3.1
- mity/md4c@release-0.5.2
- pcre2project/pcre2@pcre2-10.44
- pnggroup/libpng@v1.6.43
- qt/qtbase@04f1e432a51

intel/tinycbor@v0.6.0

Primary Language **QMake** · First Published **3 years ago** · Version Published **3 years ago** · Last Push **21 days ago** · **187** Forks · **4** Branches · **1.47 MB** Repository Size · **483** Stargazers

1 Referenced Version

intel/tinycbor@v0.6.0 Published 3 years ago

Introduced By

qtbase-04f1e432a51+dev+dirty

intel/tinycbor@v0.6.0

MIT License

Free · OSI Approved

Usage

Describes how software may be used under this license.

Commercial Use — Allowed

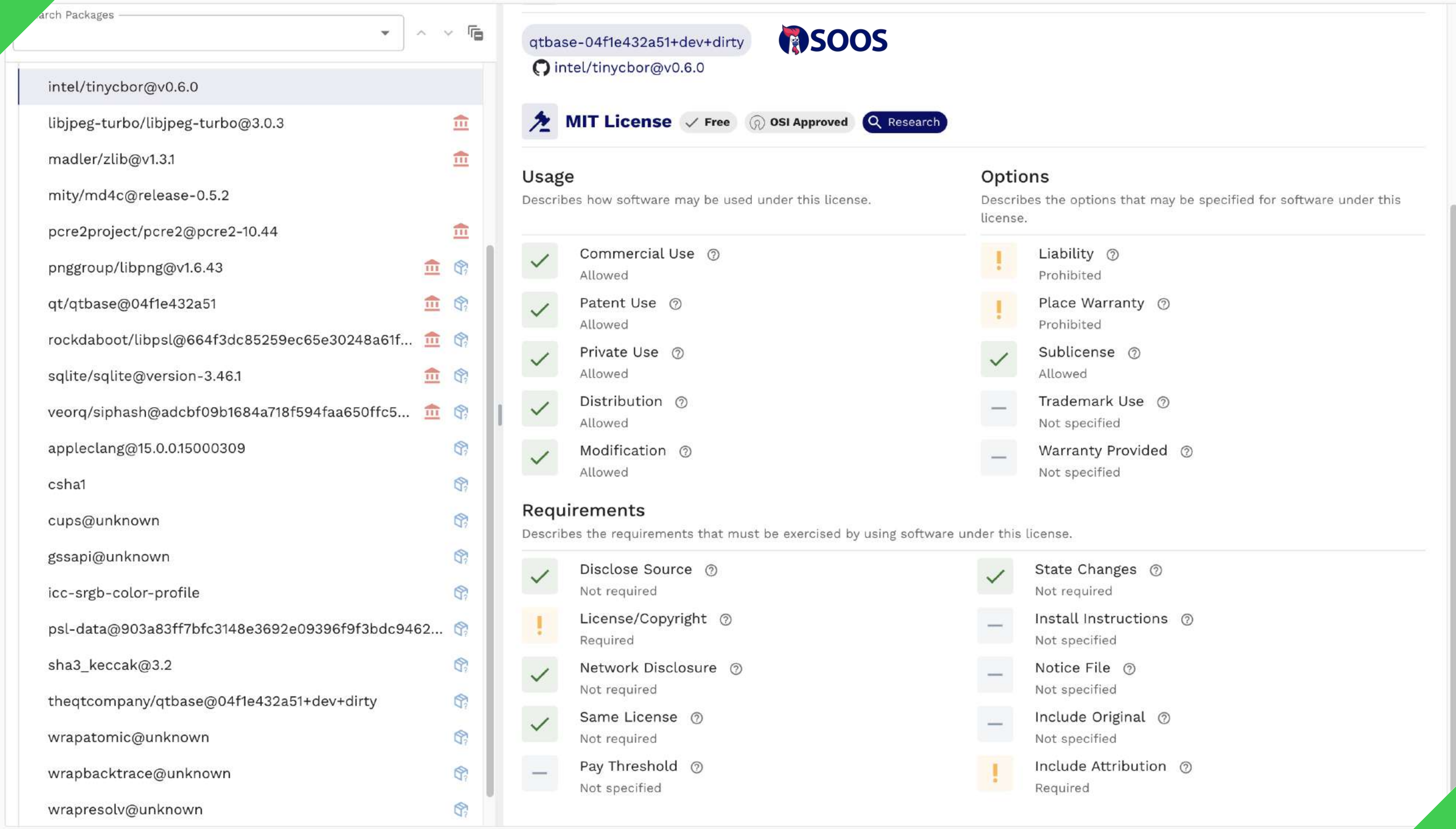
Patent Use

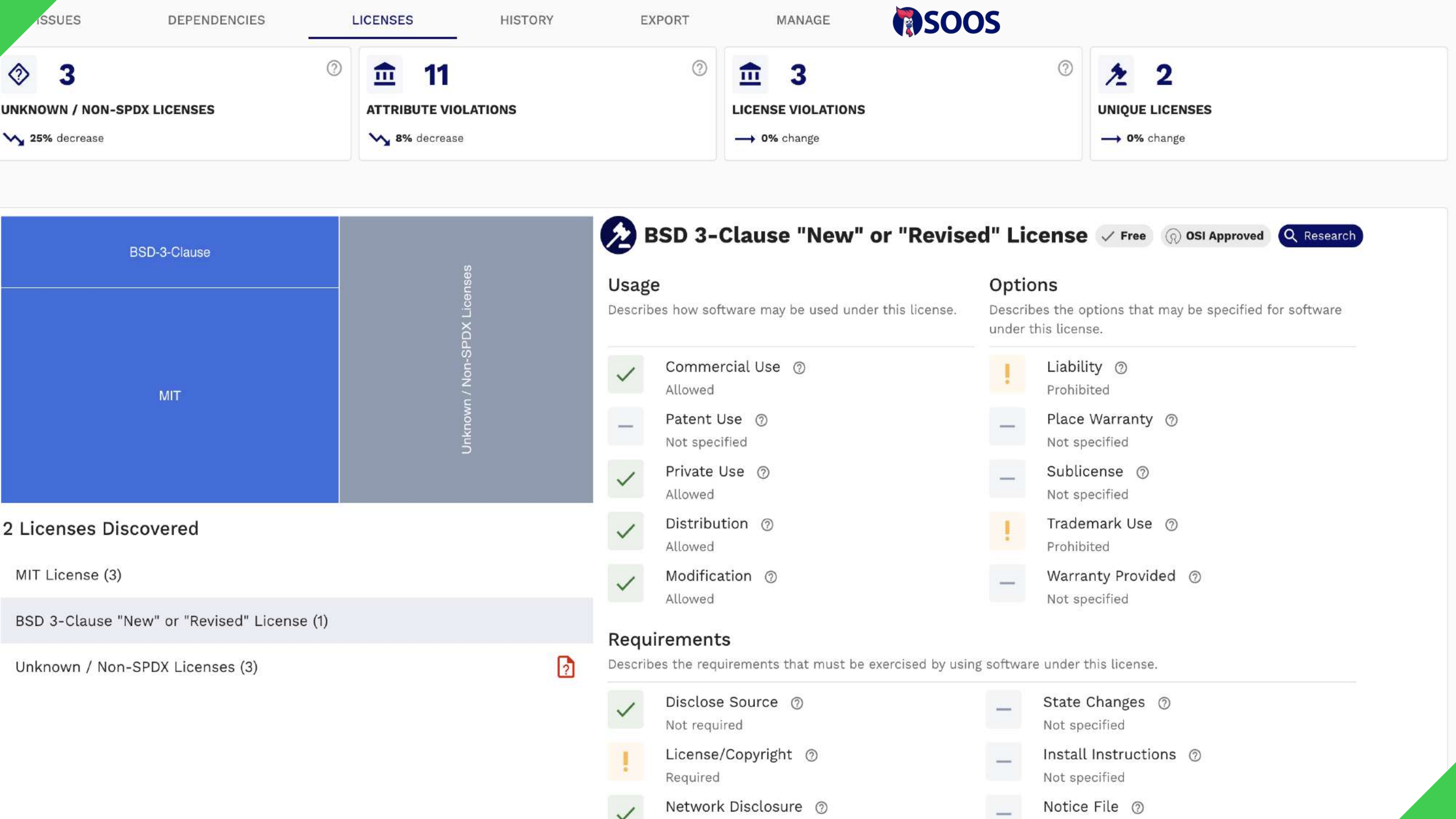
Options

Describes the options that may be specified for software under this license.

Liability — Prohibited

Place Warranty





3
UNKNOWN / NON-SPDX LICENSES
25% decrease

11
ATTRIBUTE VIOLATIONS
8% decrease

3
LICENSE VIOLATIONS
0% change

2
UNIQUE LICENSES
0% change

2 Licenses Discovered

MIT License (3)

BSD 3-Clause "New" or "Revised" License (1)

Unknown / Non-SPDX Licenses (3)

BSD 3-Clause "New" or "Revised" License

✓ Free · OSI Approved · Research

Usage

Describes how software may be used under this license.

✓ Commercial Use
Allowed

— Patent Use
Not specified

✓ Private Use
Allowed

✓ Distribution
Allowed

✓ Modification
Allowed

Options

Describes the options that may be specified for software under this license.

! Liability
Prohibited

— Place Warranty
Not specified

— Sublicense
Not specified

! Trademark Use
Prohibited

— Warranty Provided
Not specified

Requirements

Describes the requirements that must be exercised by using software under this license.

✓ Disclose Source
Not required

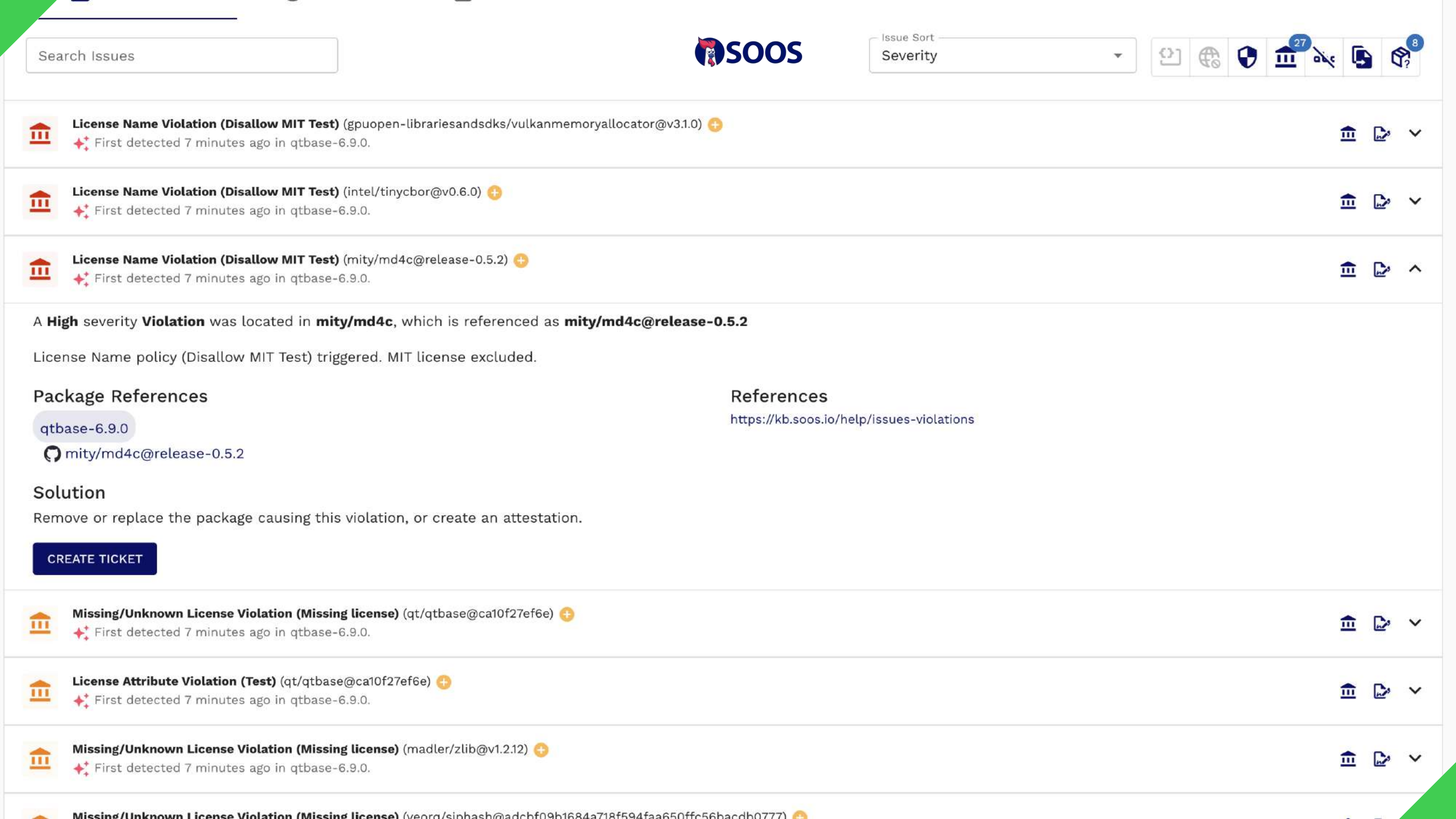
! License/Copyright
Required

✓ Network Disclosure

— State Changes
Not specified

— Install Instructions
Not specified

— Notice File



License Name Violation (Disallow MIT Test) (gpuopen-librariesandsdks/vulkanmemoryallocator@v3.1.0)
First detected 7 minutes ago in qtbase-6.9.0.

License Name Violation (Disallow MIT Test) (intel/tinycbor@v0.6.0)
First detected 7 minutes ago in qtbase-6.9.0.

License Name Violation (Disallow MIT Test) (mity/md4c@release-0.5.2)
First detected 7 minutes ago in qtbase-6.9.0.

A **High** severity **Violation** was located in **mity/md4c**, which is referenced as **mity/md4c@release-0.5.2**

License Name policy (Disallow MIT Test) triggered. MIT license excluded.

Package References

qtbase-6.9.0
mity/md4c@release-0.5.2

References

https://kb.soos.io/help/issues-violations

Solution

Remove or replace the package causing this violation, or create an attestation.

CREATE TICKET

Missing/Unknown License Violation (Missing license) (qt/qtbase@ca10f27ef6e)
First detected 7 minutes ago in qtbase-6.9.0.

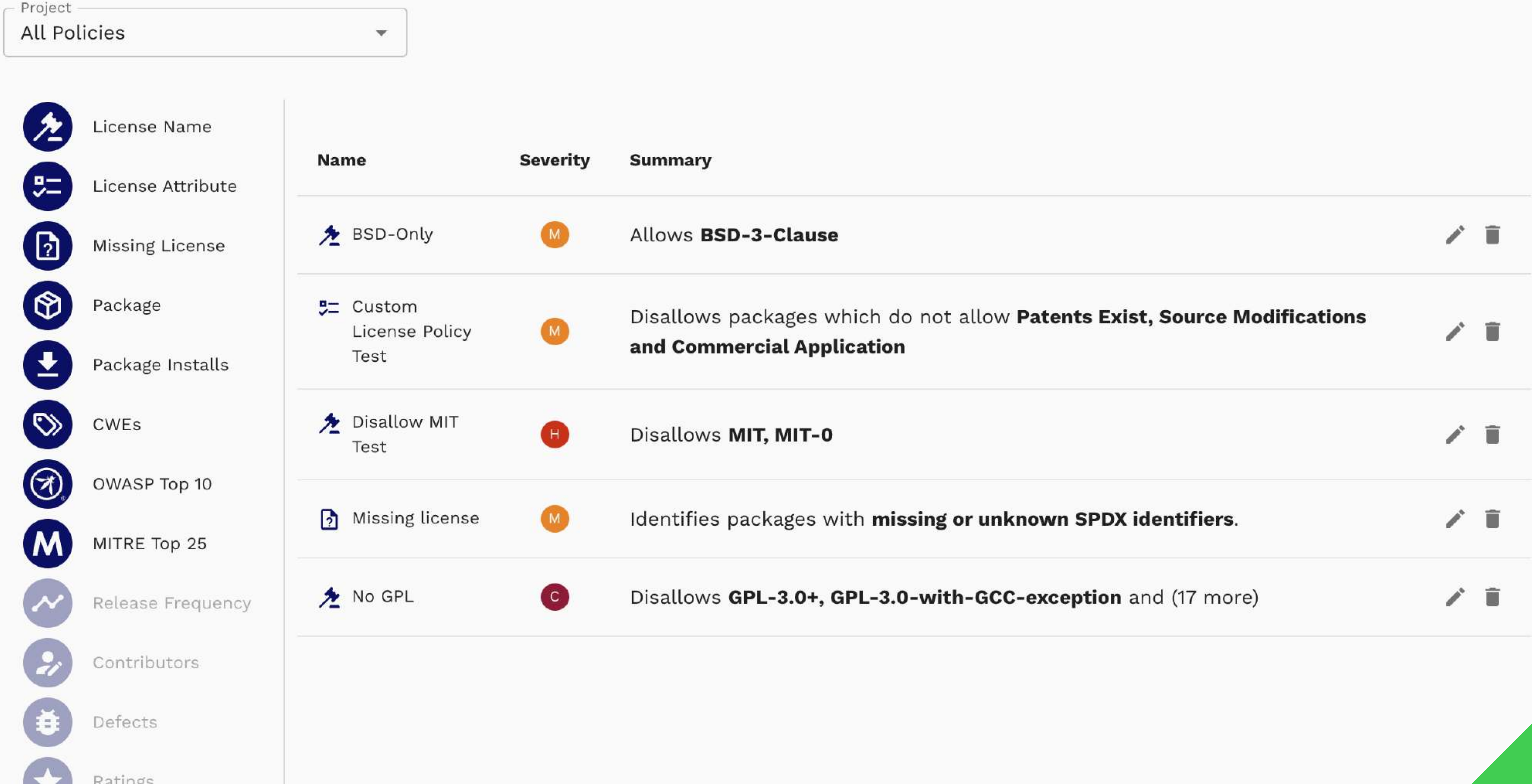
License Attribute Violation (Test) (qt/qtbase@ca10f27ef6e)
First detected 7 minutes ago in qtbase-6.9.0.

Missing/Unknown License Violation (Missing license) (madler/zlib@v1.2.12)
First detected 7 minutes ago in qtbase-6.9.0.

Missing/Unknown License Violation (Missing license) (veorg/siphash@adcbf09b1684a718f594faa650ffc56bacdb0777)

Governance

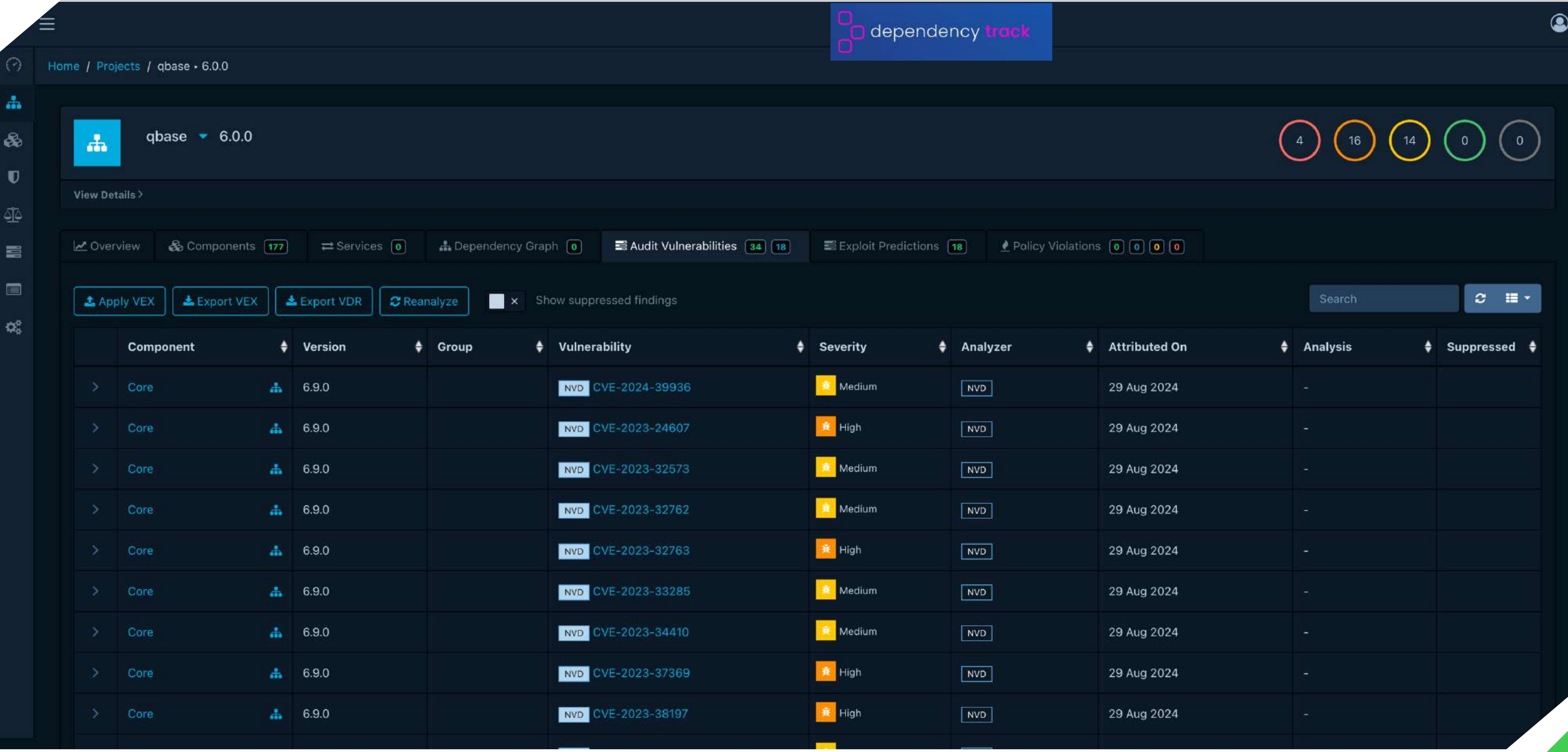
SOOS



Project: All Policies

- License Name
- License Attribute
- Missing License
- Package
- Package Installs
- CWEs
- OWASP Top 10
- MITRE Top 25
- Release Frequency
- Contributors
- Defects
- Ratings

Name	Severity	Summary
BSD-Only	M	Allows **BSD-3-Clause**
Custom License Policy Test	M	Disallows packages which do not allow **Patents Exist, Source Modifications and Commercial Application**
Disallow MIT Test	H	Disallows **MIT, MIT-0**
Missing license	M	Identifies packages with **missing or unknown SPDX identifiers**.
No GPL	C	Disallows **GPL-3.0+, GPL-3.0-with-GCC-exception** and (17 more)

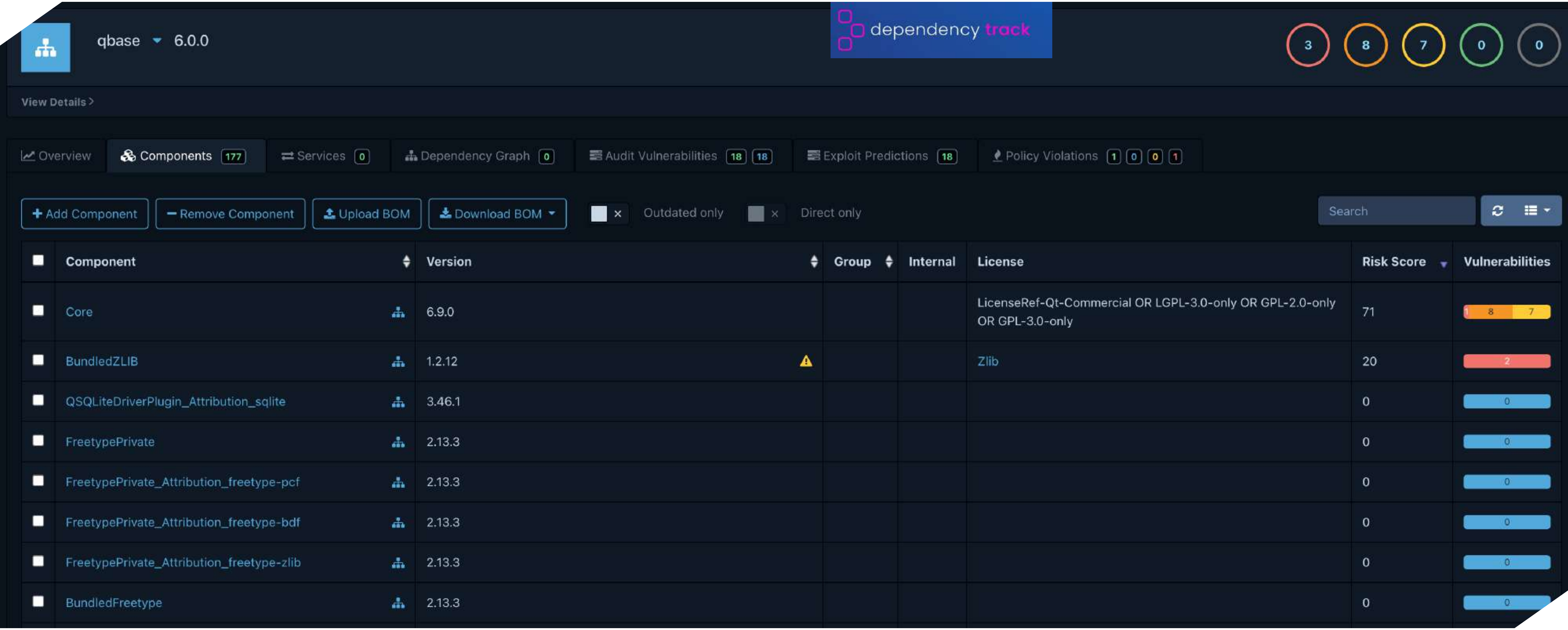


Home / Projects / qbase • 6.0.0

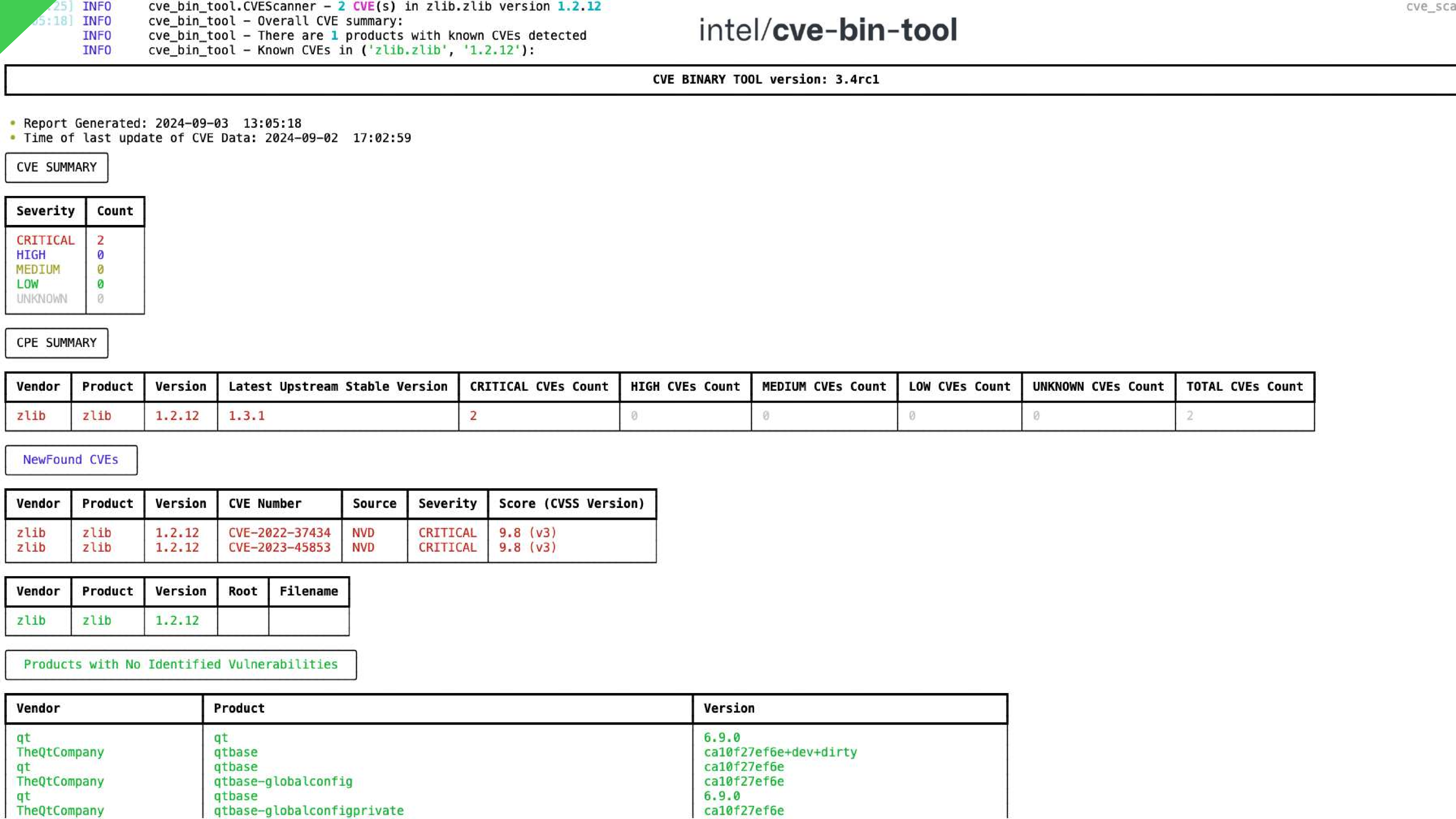
qbase 6.0.0

□ × Show suppressed findings

Component	Version	Group	Vulnerability	Severity	Analyzer	Attributed On	Analysis	Suppressed
Core	6.9.0		NVD CVE-2024-39936	Medium	NVD	29 Aug 2024	-	
Core	6.9.0		NVD CVE-2023-24607	High	NVD	29 Aug 2024	-	
Core	6.9.0		NVD CVE-2023-32573	Medium	NVD	29 Aug 2024	-	
Core	6.9.0		NVD CVE-2023-32762	Medium	NVD	29 Aug 2024	-	
Core	6.9.0		NVD CVE-2023-32763	High	NVD	29 Aug 2024	-	
Core	6.9.0		NVD CVE-2023-33285	Medium	NVD	29 Aug 2024	-	
Core	6.9.0		NVD CVE-2023-34410	Medium	NVD	29 Aug 2024	-	
Core	6.9.0		NVD CVE-2023-37369	High	NVD	29 Aug 2024	-	
Core	6.9.0		NVD CVE-2023-38197	High	NVD	29 Aug 2024	-	



□	Component	Version	Group	Internal	License	Risk Score	Vulnerabilities
□	Core	6.9.0			LicenseRef-Qt-Commercial OR LGPL-3.0-only OR GPL-2.0-only OR GPL-3.0-only	71	1 8 7
□	BundledZLIB	1.2.12 ⚠			Zlib	20	2
□	QSQLiteDriverPlugin_Attribution_sqlite	3.46.1				0	0
□	FreetypePrivate	2.13.3				0	0
□	FreetypePrivate_Attribution_freetype-pcf	2.13.3				0	0
□	FreetypePrivate_Attribution_freetype-bdf	2.13.3				0	0
□	FreetypePrivate_Attribution_freetype-zlib	2.13.3				0	0
□	BundledFreetype	2.13.3				0	0



intel/**cve-bin-tool**

```
25] INFO      cve_bin_tool.CVEScanner - 2 CVE(s) in zlib.zlib version 1.2.12
05:18] INFO      cve_bin_tool - Overall CVE summary:
       INFO      cve_bin_tool - There are 1 products with known CVEs detected
       INFO      cve_bin_tool - Known CVEs in ('zlib.zlib', '1.2.12'):
```

cve_sca

CVE BINARY TOOL version: 3.4rc1

- Report Generated: 2024-09-03 13:05:18
- Time of last update of CVE Data: 2024-09-02 17:02:59

CVE SUMMARY

Severity	Count
CRITICAL	2
HIGH	0
MEDIUM	0
LOW	0
UNKNOWN	0

CPE SUMMARY

Vendor	Product	Version	Latest Upstream Stable Version	CRITICAL CVEs Count	HIGH CVEs Count	MEDIUM CVEs Count	LOW CVEs Count	UNKNOWN CVEs Count	TOTAL CVEs Count
zlib	zlib	1.2.12	1.3.1	2	0	0	0	0	2

NewFound CVEs

Vendor	Product	Version	CVE Number	Source	Severity	Score (CVSS Version)
zlib	zlib	1.2.12	CVE-2022-37434	NVD	CRITICAL	9.8 (v3)
zlib	zlib	1.2.12	CVE-2023-45853	NVD	CRITICAL	9.8 (v3)

Vendor	Product	Version	Root	Filename
zlib	zlib	1.2.12		

Products with No Identified Vulnerabilities

Vendor	Product	Version
qt	qt	6.9.0
TheQtCompany	qtbase	ca10f27ef6e+dev+dirty
qt	qtbase	ca10f27ef6e
TheQtCompany	qtbase-globalconfig	ca10f27ef6e
qt	qtbase	6.9.0
TheQtCompany	qtbase-globalconfigprivate	ca10f27ef6e

Ongoing and future work

© The Qt Company

Future work

- Finalize Qt Source SBOM <- ongoing

- Build SBOM
  - Qt WebEngine
  - Tools (e.g. Qt Creator)
  - qttranslations <- ongoing

- SBOM creation for User projects – Very rough PoC available

- Look into SBOM tooling
  - Dependency and Vulnerability Monitoring
  - Reporting

Thanks

@alcroito on #qt-cmake @ irc.libera.chat (bridged to kde.org matrix server)